IN THE DISTRICT COURT OF THE UNITED STATES
DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

UNITED STATES OF AMERICA v. AMIR GOLESTAN MICFO, LLC	Crim. No. 2:19-cr-00441-RMG **GOVERNMENT'S MEMORANDUM PERTAINING TO CALCULATION OF LOSS**

Pursuant to the Court's Order dated November 18, 2021, The United States of America, through its undersigned attorneys, hereby submits this Memorandum setting forth its calculation of loss and the legal and factual basis for its calculation.

FACTS PERTINENT TO LOSS CALCULATION

Defendants Amir Golestan (Golestan) and Micfo, LLC (Micfo) (collectively, Defendants) pled guilty on November 16, 2021 to twenty counts of wire fraud pursuant to 18 U.S.C. § 1343. ECF No. 105. Defendants' guilty pleas were entered after 1.5 days of trial. Defendants pled guilty to devising a scheme and artifice to defraud and obtain property, specifically IPv4 addresses from the American Registry for Internet Numbers (ARIN), by means of false and fraudulent representations.

Defendants fraudulently obtained IPv4 address rights in two ways. In each instance, Defendants created and utilized Channel Partner companies[1] to obtain the rights to IP addresses that they could not legally obtain. The Channel Partner companies purported to be individual businesses, and Golestan created fictitious persons as the presidents and directors of each of the Channel Partner companies. Initially, Defendants used the Channel Partner companies as a false

[1] The following Channel Partner companies were created by Defendants: (1) Contina; (2) Virtuzo; (3) Oppobox; (4) Telentia; (5) Univera Network/HostAware; (6) Roya Hosting; (7) Host Bang; (8) Hyper VPN; (9) Fiber Galaxy; and (10) Cloudiac.

justification for Micfo's need for IPv4 addresses. After this initial avenue of fraudulently obtaining IPv4 addresses, Defendants began to apply to ARIN on behalf of the Channel Partner companies themselves for IPv4 addresses. The Channel Partner companies purported to be individual businesses, which required IP addresses, and would apply directly to ARIN for the IP addresses. Specifically, the Channel Partners would complete paperwork, which included the identification of officers, and provide justification for the Channel Partner's need for IP addresses. Golestan created fictitious persons as officers for each Channel Partner company, and at times falsely claimed a need or justification for IP addresses using these fictitious persons and companies.

John Sweeting, Chief Consumer Officer for ARIN and Former Elected Chairman of the ARIN Advisory Council, testified at trial regarding the fraudulently obtained IPv4 addresses. Based on Sweeting's testimony and the evidence admitted at trial, without objection, Defendants successfully obtained 1,077,130 IPv4 addresses based on either partial or completely fraudulent representations.[2] Moreover, in September 2014, Defendants attempted to acquire an additional 262,142 IPv4 addresses, but this attempted acquisition was flagged by ARIN and never was completed. The total number of IPv4 addresses that Defendants fraudulently obtained or attempted to obtain is 1,339,272. These figures are discussed in more detail later in this memorandum.

As presented at trial, the demand for IPv4 addresses has become significant since ARIN's free pool of addresses is now depleted. As a result of the demand for IPv4 addresses, a secondary market exists for the transfer of IP addresses. Brokers are often used to facilitate the sale and transfer of IP addresses between businesses. Brokerage companies that were involved in the sale

[2] Sweeting testified at trial that IPv4 addresses obtained by Micfo using fictitious Channel Partners were obtained wholly by fraud. Even if legitimate justifications existed apart from the false Channel Partner information, ARIN would not have granted the fictitious Channel Partner rights to the IPv4 addresses.

of Defendants' fraudulently obtained IPv4 addresses were: Hilco Streambank, Nationwide Computer Systems, Inc., Cheval Capital, and IPv4 Market Group. The Court heard testimony from the following brokers at trial: Jack Hazan, Mike Burns, Hillary Stiff, and IPv4 Market Group. Each broker that testified explained the demand for IPv4 addresses and the increasing value of an IPv4 address. In 2017, the market rate for an IP address ranged from $9 to $13. At the time Defendants' fraud was discovered, IPv4 addresses were selling for between $17 to $19 an address. Currently, market rates for an IPv4 addresses are around $50 an address.

Defendants' fraudulent scheme ran from 2017 to the fall of 2018 when his fraud was discovered by ARIN. The value of the IPv4 address blocks that Defendants fraudulently obtained in some instances can be readily determined, since they were either sold or under contract for sale. In other instances, a range needs to be used. The Government has attached as Exhibit 1 to this Memorandum, a chart that lists the following:

a. The Company (Micfo or a Channel Partner Company) that had the rights to the IP address block.[3]

b. The range for the IP address block.

c. The total number of IP addresses in the block.

d. In the case of a completed or attempted sale: Column F lists the trial exhibit that evidences the completed or attempted sale, Column G lists the price per IP address, and Column I list the purchase price for each completed or attempted contract.

e. Column H is a column that indicates whether the IP address block was listed as part of the attempted Amazon contract and if the IP address block was not part of another transaction, Column I lists the purchase price at $15.50 an address.

[3] If the Company is Micfo, the Channel Partners used as justification are listed in Column E of Exhibit 1.

f. Column J lists the range of loss amount for the non-listed IPv4 addresses and the attempted IPv4 address block Defendants attempted to obtain in September 2014.

ARGUMENT

When a defendant pleads guilty or is convicted of a fraud offense, including wire fraud pursuant to 18 U.S.C. § 1343, the United States Sentencing Commission's Guidelines Manual directs that the appropriate chapter and section to guide sentencing is § 2B1.1. *United States Sentencing Commission Guidelines Manual*, App'x A.[4] Pursuant to § 2B1.1, a defendant's base offense level increases depending on the specific loss amount at issue. *Id.*, § 2B1.1(b). The United States Sentencing Commission in Note 3 to § 2B1.1 has given sentencing courts guidance on how to calculate loss for the purposes of § 2B1.1(b).

As a general rule, loss is the greater of "actual" or "intended" loss. *Id.* at n. 3(A). "Actual" loss means the "reasonably foreseeable pecuniary harm that resulted from the offense." *Id.* at n. 3(A)(i). "Intended" loss means "(I) the pecuniary harm that the defendant purposefully sought to inflict; and (II) includes intended pecuniary harm that would have been impossible or unlikely to occur." *Id.* at n. 3(A)(ii). Further, "both charged and uncharged conduct may be considered." *United States v. Anderson*, 532 F. App'x. 373, 380 (4th Cir. 2013). "Pecuniary harm" means "harm that is monetary or that otherwise is readily measurable in money," and "reasonably foreseeable pecuniary harm" means "pecuniary harm that the defendant knew or, under the circumstances, reasonably should have known was a potential result of the offense." § 2B1.1 n. (A)(iii)–(iv).

[4] Appendix A also references § 2C1.1; however, this section pertains to Offenses Involving Public Officials and is, therefore, not applicable to the present case.

Despite the general rule that a court must determine which is greater – the actual loss or intended loss – the actual loss and intended loss are not mutually exclusive and may be combined to calculate overall intended loss. *See United States v. Sesay*, 937 F.3d 1146, 1153 (8th Cir. 2019) (finding that the district court properly included the actual loss suffered with the total intended loss for the purposes of determining loss amount under §2B1.1); *see also United States v. Ware*, 334 F. App'x. 49, 50-51 (8th Cir. 2009) (finding that intended loss includes both actual losses and the intended loss from the fraud).

Importantly, the sentencing court "need only make a reasonable estimate of the loss." *Id.* n. 3(C); *see also United States v. Stone*, 866 F.3d 219, 228 (4th Cir. 2017) (holding that the sentencing court need only make a reasonable estimation of loss and that the sentencing judge is in a unique position to assess the evidence). The Sentencing Commission has listed several factors to consider when making the estimate. Pertinent to the present case is "the fair market value of the property unlawfully taken."[5] § 2B1.1 n.3(C)(i). The Government must prove the amount of loss by a preponderance of evidence, and the district court must "make a reasonable estimate of

[5] When determining the "intended loss," a court is not required to determine or analyze who the victims of the fraud were and/or the number of victims as it is not part of the "intended loss" estimation. The pertinent analysis focuses on the loss that the "***defendant was intending to inflict.***" § 2B1.1 at n.3(A)(ii). In note 3(C)(iv), the Sentencing Commission does state that the "approximate number of victims multiplied by the average loss to each victim" is a factor the sentencing court can consider. However, in the present case, the more readily ascertainable factor in estimating loss is a determination of the fair market value of the property unlawfully taken. *See* §2B1.1 at n.3(C)(i). This is further established by the separate number of victims enhancement found in § 2B1.1(b)(2). *See also Anderson*, 532 F. App'x at 379 (noting the distinction between the number of victims enhancement and the intended loss calculation). Should the Court determine that an analysis of the number of victims in pertinent, the primary victim of Defendants' fraud is ARIN. Moreover, the loss to ARIN, despite the fact that it would not have realized the dollar amount for each IPv4 address, is the value of each IPv4 address because Defendants' fraud took away ARINs ability to issue the IPv4 address to a legitimate business or entity.

the loss, given the available information." *United States v. Miller*, 316 F.3d 495, 503 (4th Cir. 2003).

As will be discussed in more detail below, based on the fair market value of the IPv4 addresses during the time the Defendants perpetrated their fraud on ARIN, the Government is able to prove an intended loss amount that ranges between $19,067,512 – $23,203,952 by a preponderance of the evidence.

I. Law pertaining to intended loss.

It is well-established in the Fourth Circuit that "loss" is not limited to actual loss and can be calculated using the defendant's "intended loss." *See Miller*, 316 F.3d at 499 (4th Cir. 2003) (rejecting the defendant's argument that the Guidelines limits loss to actual, rather than intended loss); *see also United States v. Brothers Constr. Co.,* 219 F.3d 300, 318 (4th Cir.2000) ("[I]f an intended loss that the defendant was attempting to inflict can be determined, this figure will be used if it is greater than the actual loss."). Moreover, the Guidelines permit courts "to find intended loss in an amount exceeding that which was in fact possible or probable." *Miller*, 316 F.3d at 501. The Fourth Circuit has adopted this majority view on intended loss calculation finding that it is consistent with the Sentencing Commission's goal that the "defendant's intent be the focal point of the guideline." *Id.* at 502. This view is "consistent with the important principle underlying the Guidelines, namely matching punishment with culpability." *Id.* at 502-03; *see also United States v. Studevent,* 116 F.3d 1559, 1563 (D.C.Cir.1997) ("limiting intended loss to that which is likely or possible … would eliminate the distinction between a defendant whose only ambition was to make some pocket change and one who plotted a million-dollar fraud.").

A Seventh Circuit Court of Appeals case is instructive to the analysis in the present case. In *United States v. Sliman,* 449 F.3d 797 (7th Cir. 2006), Sliman and his co-defendants were part

of scheme that would enable them to receive cash from financial institutions by depositing counterfeit checks. 449 F.3d at 798-99. To further the scheme, a counterfeit "check factory" was operated out of an apartment in Illinois. *Id.* at 799. When police executed a search warrant on the apartment, a "check register" was found on a computer indicating that counterfeit checks worth $36,900,000 had been produced with and printed from the computer. [6] *Id.* The $16 million in checks made payable to RVAL was pertinent to the sentencing analysis because it consisted of "four batches" of checks totaling $ 4 million each. *Id.* The first two of checks—$8 million total —were intercepted by customs without the various defendant's knowledge. *Id.* The remaining third batch was negotiated, except for $1 million that was recovered by customs, and the fourth batch was recovered when one of the co-defendants was arrested. *Id.*

In reaching its conclusion that the intended loss was approximately $26 million, the district court included the value of all counterfeit checks on the check register found during the search of the apartment. *Id.* at 802.[7] Sliman argued that the intended loss was $4 million because it took into account the various co-conspirators four attempts to produce one batch of counterfeit checks. *Id.* at 803. The Seventh Circuit Court of Appeals found that the district court properly calculated the intended loss by including all counterfeit checks on the check register found because that was the amount of loss the conspiracy intended to bring about. *See Id.* at 801, 803.

[6] "Approximately $9 million worth of the checks listed on the register were found on the floor of the apartment torn into pieces. Of the remaining approximately $28 million in checks, $2 million were printed before Sliman joined the conspiracy. Of the $26 million in intact checks printed during the time Sliman participated in the conspiracy, approximately $16 million worth were made payable to RVAL. The remaining checks, totaling approximately $10 million, were made payable to aliases of Sliman, Dacca, and Salama." *Sliman*, 499 F.3d at 799.

[7] The district court subtracted the $9 million in torn up checks and $2 million in checks that were printed before Sliman joined the conspiracy.

II. Loss calculation based on Defendants IPv4 addresses Defendants obtained or attempted to obtain fraudulently.

As was evidenced through nearly a full day of testimony at trial, the Defendants fraud was complete once ARIN issued the fraudulently obtained IPv4 addresses. The value of the total amount of IPv4 addresses that Defendants obtained, or attempted to obtain, is the total intended loss. *See* §2B1.1, n. 3(A)(ii). Moreover, the testimony and evidence admitted through the four broker witnesses established that Defendants were actively seeking to sell the fraudulently obtained IPv4 addresses and realize the value from their criminally obtained property.

The Court need only make a reasonable estimation of the value of the intended loss. As was outlined above, the Defendants perpetuated their fraud on ARIN from 2017 to the fall of 2018. The value of the IPv4 addresses ranged from $9 an address in 2017 to $19 an address in fall 2018. Defendants fraudulently obtained or attempted to obtain a total of 1,343,366 IPv4 addresses from ARIN, and the Fourth Circuit has made it clear that "both charged and uncharged conduct may be considered" at sentencing. *See Anderson*, 532 F. App'x. at 380. As the notes to the §2B1.1 set forth, the "fair market value of the property unlawfully taken" is a factor the court can consider when estimating loss. §2B1.1 at n.3(C)(i).

To fully ascertain the loss amount for the 1,339,272 addresses, it is necessary to divide the addresses into four categories: (1) IPv4 address blocks successfully sold prior to Defendants' fraud being discovered; (2) IPv4 address blocks under contract when Defendants' fraud was discovered; (3) IPv4 address blocks under preliminary contract with Amazon; (4) IPv4 addresses not sold or under any type of contract; and (5) IPv4 addresses that Defendants attempted to gain by fraud. Once a value is ascertained for each category, the total intended loss is **$**19,067,512 – $23,203,952. As described at trial, and reflected in the attached Exhibit 1, the amounts corresponding to these categories are:

1. IPv4 address blocks successfully sold prior to Defendants' fraud being discovered.

   a. Tencent: three IPv4 address blocks at $9 an address for $589,824.00.[8]

   b. NTTPC: two IPv4 address blocks at $17 an address for $1,671,168.00.[9]

   c. Bahnhof: one IPv4 address block at $17 an address for $1,114,112.00.00.[10]

The total of these three contracts is $3,375,104 (hereinafter referred to as the Completed Transactions).

2. IPv4 address blocks under contract when Defendants' fraud was discovered.

At the time Golestan's fraud was discovered by ARIN, he had an Asset Purchase Agreement with Saudi Telecom to sell seven address blocks at $19 an address (hereinafter referred to as the Saudi Telecom Transaction). The total purchase price for the Saudi Telecom Transaction was $6,225,920.00.

Golestan also had agreed to sell to CUBL an IPv4 address block for $19 an address. The total purchase price for this transaction was $155,818.

3. IPv4 address blocks under preliminary contract with Amazon.

As was presented at trial through Hillary Stiff of Cheval Capital, in April 2018 Defendants were in negotiations to sell 913,408 IPv4 addresses to Amazon.[11] Amazon had agreed to purchase these IPv4 address rights for $15.50 an address, for a total of $14,157,824.00.

[8] The Government would refer the Court to its trial exhibit number 72.
[9] The Government would refer the Court to its trial exhibit number 68.
[10] The Government would refer the Court to its trial exhibit number 69.
[11] The Government would refer the Court to its trial exhibit number 79.

Of the total IPv4 address blocks listed for sale to Amazon, 11 address blocks were sold as part of the Completed Transactions or were included in the Saudi Telecom Transaction or CUBL transaction; as a result, there is an alternate value assigned to these addresses.[12]

After subtracting out the blocks that have an alternate value assigned to them, 20 IPv4 address blocks remain, equaling 360,508 IPv4 addresses.[13] At a value of $15.50, these addresses represent a total of $5,587,874.

4. IPv4 addresses not sold or under any type of contract.

Golestan also had several IPv4 address blocks that were obtained fraudulently but never under contract. As seen in Exhibit 1, these total 151,502 addresses.[14] Using a range of $9 - $19 results in a total value range of $1,363,518 - $2,878,538.

5. IPv4 addresses that Defendants attempted to gain by fraud.

As John Sweeting testified at trial, in September 2014 Golestan attempted to obtain a /14 block fraudulently but was stopped by ARIN. This block consisted of 262,142 IPv4 addresses and using a range of $9 - $19 had a value of $2,359,278 - $4,980,698.[15]

[12] The 11 IPv4 address blocks that have an alternate value are as follows: (1) 23.232.128.0/17 (Exhibit 1, row 4 – NTPCC Contract); (2) 23.247.128.0/17 (Exhibit 1, row 5 – Saudi Telecom Transaction); (3) 107.153.0.0/16 (Exhibit 1, row 6 – NTPCC Contract); (4) 107.168.0.0/15 (Exhibit 1, row 7 – Saudi Telecom Transaction); (5) 45.45.128.0/17 (Exhibit 1, row 12 – Saudi Telecom Transaction); (6) 172.82.0.0/17 (Exhibit 1, row 13 – Saudi Telecom Transaction); (7) 98.128.0.0/16 (Exhibit 1, row 14 – Bahnoff Contract); (8) 104.247.0.0/19 (Exhibit 1, row 16 – CUBL attempted Transaction); (9) 64.112.0.0/17 (Exhibit 1, row 18 – Saudi Telecom Transaction); (10) 45.42.128.0/17 (Exhibit 1, row 29– Saudi Telecom Transaction); (11) 172.99.128.0/17 (Exhibit 1, row 30 – Saudi Telecom Transaction).

[13] These remaining IPv4 address blocks are identified on Exhibit 1 with a light peach highlight.

[14] These IPv4 addresses are identified on Exhibit 1 with light green highlight.

[15] These IPv4 addresses are identified on Exhibit 1 with light blue highlight.

6. Total intended loss.

Adding up these amounts results in the following total:

A.	Contracts paid:	$3,375,104
B.	Contracts stopped:	$6,381,738
C.	Amazon contract remaining:	$5,587,874
D.	Not under any contract:	$1,363,518 - $2,878,538
E.	Attempted to obtain:	$2,359,278 - $4,980,698
	Total:	**$19,067,512 – $23,203,952**

CONCLUSION

As set forth herein, based on the fair market value of the IPv4 addresses during the time the Defendants perpetrated their fraud on ARIN, the Government can prove by a preponderance of the evidence an intended loss amount that ranges between $19,067,512 – $23,203,952**.**

Respectfully submitted,

M. RHETT DEHART
ACTING UNITED STATES ATTORNEY

BY: *s/Amy Bower*
NATHAN S. WILLIAMS (ID#10400)
AMY F. BOWER (ID#11784)
Assistant United States Attorneys
151 Meeting Street, Suite 200
Charleston, SC 29401
843-727-4381

December 3, 2021
Charleston, South Carolina